# AUTOMOX

# AUTOMOX ENDPOINT HARDENING: CROSS-PLATFORM, GLOBALLY ACCESSIBLE CYBER HYGIENE AT SCALE

**Automated Patch Management**
Continuous patching of OS and third-party applications

**Automox Worklets™**
Create custom tasks using scripts across any managed Windows, macOS, or Linux device

**Cloud-Native Platform**
Harden endpoints without complex infrastructure or VPN requirements

**Configuration Management**
Serverless configuration management for all managed devices with zero drift

**Continuous Policy Enforcement**
Automatically enforce patching, configuration, deployment, and Automox Worklet tasks

**Cross-OS Support**
Support for Windows, macOS, and Linux devices

**Endpoint Visibility**
In-depth visibility to identify non-compliant devices

**Lightweight Agent**
Efficient and lightweight agent under 20MB

**Role-Based Access Control**
Set individual permissions for users and groups with RBAC

**Rich API**
Fully featured and documented API for complete integration into your infrastructure

**Software Deployment**
Painlessly deploy, manage, and enforce OS and third-party applications globally
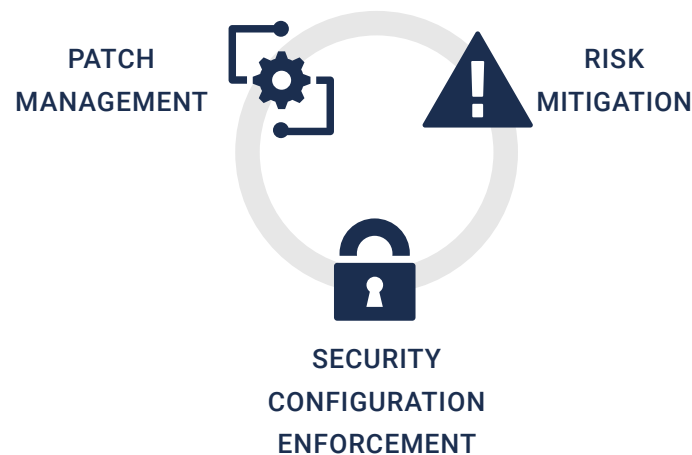
**Straightforward Reporting**
Real-time, up-to-date reports

Remote users, multi-OS environments, and diverse third-party software needs are the norm for businesses today and the ability to support these evolving, complicated environments is falling on IT teams with limited resources.

While these environments are changing and facing growing threats, these same IT teams are also tasked with minimizing and mitigating their exposure to vulnerabilities. As a result, many businesses have adopted multiple tools that require heavy training, dedicated on-site resources, with multiple dashboards to try and stay ahead.

**The next generation of endpoint hardening platforms must provide the capabilities needed at speed while meeting the endpoint hardening needs. These platforms must address:**
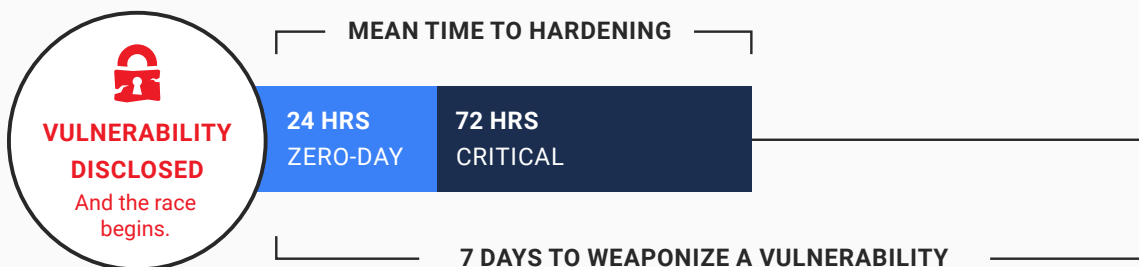
PATCH MANAGEMENT

RISK MITIGATION

SECURITY CONFIGURATION ENFORCEMENT

ALL WHILE REQUIRING LESS TIME TO COMPLETE THESE NEEDS FROM A SINGLE CONSOLE.

# Be A Smaller Target™: Automox Endpoint Hardening

**Cloud-native and globally available, Automox Endpoint Hardening enforces OS and third-party patch management, security configurations, and custom scripting across all managed devices from a single, intuitive console. Automox enables IT teams to scale with the growth and needs of the company through automated toolsets, from patch management to configuration enforcement. IT teams also have in-depth visibility of on-prem, remote, and virtual endpoints without the need to deploy costly infrastructure.**

The Automox Endpoint Hardening platform requires no infrastructure to maintain. The cloud-native console gives an administrator in-depth visibility and inventory assessments of endpoints. Capable of managing Windows, macOS, and Linux, the intuitive automation workflow is consistent across OS platforms and dramatically reduces the effort, time, and complexity of cyber hygiene automation. The lightweight agent does not require a VPN or custom configuration for remote management, and with the automation capabilities and Automox Worklets™, administrators can enforce broad, fundamental hygiene across all managed devices.

# Move faster than your adversaries with automated patching and configuration management



MEAN TIME TO HARDENING

VULNERABILITY DISCLOSED
And the race begins.

**24 HRS** ZERO-DAY

**72 HRS** CRITICAL

7 DAYS TO WEAPONIZE A VULNERABILITY

According to leading industry data, adversaries are weaponizing new critical vulnerabilities in seven days on average. Zero-day vulnerabilities are already weaponized at the moment of disclosure. To stay ahead of adversaries means you need to be remediating critical vulnerabilities within 72 hours, and zero-day vulnerabilities within 24 hours. The 24/72 endpoint hardening threshold is a new benchmark in cybersecurity, and it's time to join Automox customers who are breaking through this performance barrier.

**With Automox, you can automate policies and groups that enable you to harden your endpoints faster than adversaries can exploit vulnerabilities.**
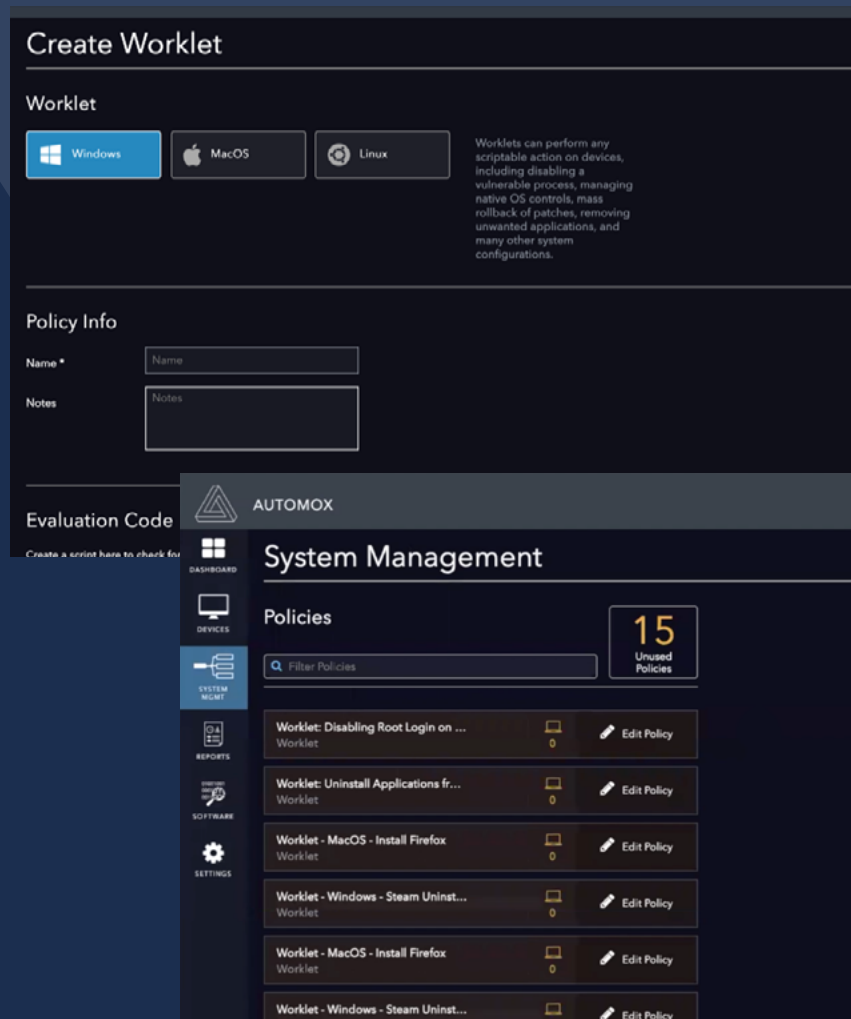
Our patch management platform provides visibility into the status of your corporate endpoints and allows the customization and automation of both OS and third-party application updates or patches to eliminate this threat vector. With policies you can patch all, include/exclude, or set up advanced rules for which OS and software is patched. You also can use patch severity levels to automate critical patches and limit cosmetic updates.

With our automated patching and configuration management, you have the confidence that you require to know all critical vulnerabilities are patched and updated across all your corporate endpoints.

## Accomplish any task that can be scripted: Automox Worklets

Automox empowers IT teams to act on any vulnerability discovered within their environments to proactively eliminate exposure before those vulnerabilities can be weaponized. With the extensible, automation architecture of Automox, customers can leverage Automox Worklets to assist in coordinated response actions.

With Automox Worklets, an IT administrator can start mitigation within minutes of discovery of a vulnerability. These worklets are reusable, script-based modules that provide the distributed capability to modify registry keys, enforce local policies, deploy and remove software and disable unwanted processes. Automox Worklets can be shared with peers and applied across Windows, Linux, and macOS devices.

# About Automox

**Facing growing threats and a rapidly expanding attack surface, understaffed and alert-fatigued organizations need more efficient ways to eliminate their exposure to vulnerabilities. Automox is a modern cyber hygiene platform that closes aperture of attack by more than 80% with just half the effort of traditional solutions.**

Cloud-native and globally available, Automox enforces OS and third-party patch management, security configurations, and custom scripting across Windows, macOS, and Linux from a single intuitive console. IT and SecOps can quickly gain control and share visibility of on-prem, remote, and virtual endpoints without the need to deploy costly infrastructure.

Experience modern, cloud-native patch management today with a 15-day free trial of Automox and start recapturing more than half the time you're currently spending on managing your attack surface. Automox dramatically reduces corporate risk while raising operational efficiency to deliver best-in-class security outcomes, faster and with fewer resources.

## Ready to get started?
## Try Automox for yourself.

Get a free 15-day trial to see why Automox is the leading cloud-native endpoint hardening solution. Sign up today!

**automox.com/signup**

△ AUTOMOX